water industry commission FOR SCOTLAND

WATER INDUSTRY COMMISSION FOR SCOTLAND

RECORDS MANAGEMENT PLAN

Submitted in accordance with the Public Records (Scotland) Act 2011

Contents

water industry
commission
FOR SCOTLAND

Covering Statement

I am pleased to submit Water Industry Commission for Scotland’s (The Commission) records management plan (RMP) for assessment by the Keeper of the Records of Scotland.

The Commission recognises its duties under the Public Records (Scotland) Act 2011 and is aware that The Act requires the Commission, and other named authorities, to prepare and implement a records management plan. Such RMP needs to provide evidence that it has proper and effective arrangements in place for the management of its records, for submission to the Keeper of the Records of Scotland.

The Commission is very much aware of the definition of a record contained in the PSRA, which includes records held in electronic and manual form, and on a range of media. While many of the Commission’s records are held electronically, paper copies are also produced and stored. This document details the arrangements in place for the management of records within the Commission, regardless of the form they take.

Our Records Management Plan is based on the Keeper’s model plan and includes the 14 elements, backed up with evidence of our compliance against each. We hope to demonstrate our commitment to continuous improvement where we feel our current practice is not robust.

Implementation of this RMP will enable The Commission to ensure compliance with the Public Records (Scotland) Act 2011, Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002.

Katherine Russell

Katherine Russell
Director of Corporate Affairs & Strategy
Water Industry Commission for Scotland

Element 1: Senior Management Responsibility

Identify a person at senior management level who has overall strategic responsibility for records management. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 (2) (a) (i).

Although Alan Sutherland is the Chief Executive and Accountable Officer for the Water Industry Commission for Scotland, our Director of Corporate Affairs and Strategy, Katherine Russell, has overall responsibility for Records Management. The responsibility for records management has been delegated to Kirsty McLean.

Any enquiries about WICS records management should be routed through: enquiries@watercommission.co.uk or, alternatively, can be addressed to:

Water Industry Commission for Scotland
First Floor, Moray House
Forthside Way
Stirling
FK8 1QZ

Element 2: Records Manager Responsibility

Identify an individual within the organisation, answerable to senior management, to have operational responsibility for records management within the organisation. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 (2) (a) (ii).

Kirsty McLean, Finance Officer & PA, has operational responsibility for records management within The Commission. Her role includes the development and implementation of the RMP and she will be the first point of contact for the National Records of Scotland. Kirsty will work as part of a small team called the Records Management Working Group, consisting of another two members.

Any enquiries relating to the operational aspects of records management should be routed through: enquiries@watercommission.co.uk or, alternatively, can be addressed to:

Water Industry Commission for Scotland
First Floor, Moray House
Forthside Way
Stirling
FK8 1QZ

Element 3: Records Management Policy Statement

A records management policy statement underpins effective management of an authority's records and information. It demonstrates to employees and stakeholders that managing records is important to the authority and serves as a mandate for the activities of the records manager. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 2) (b) (i).

Why the Commission has a records management code of practice

Section 61 of the Freedom of Information (Scotland) Act 2002 requires Scottish Ministers to issue a code of practice to Scottish public authorities as to the practice which it would, in the opinion of the Ministers, be desirable for the authorities to follow in connection with the keeping, management and destruction of the authorities' records. In exercising their functions under section 61, Ministers are to have regard to the public interest in allowing public access to information held by Scottish Public authorities.

The Scottish Government has issued a draft code of practice for public bodies in Scotland which has to form the basis of The Commission's code of practice on records management.

The Commission is also subject to the Public Records (Scotland) Act 2011 which requires specific public bodies to set out proper arrangements for the management of its records.

Aims of the records management code of practice

The aims of the code are:

- To set out practices which should be followed in relation to the creation, keeping, management and final disposition of all records;
- To determine a criteria of records;
- To establish a list of legally required records and the duration for which they must be held;
- To establish a maximum period for which records should be held;
- To establish the arrangements for the final disposition of records or record transfer to the National Archives of Scotland is appropriate.

Preparation for the commission's code of practice

In formulating this code of practice, The Commission has had regard to the guidance issued by Scottish Ministers and in particular the Model Action Plan (MAP), produced by the National Records of Scotland and published by the Scottish Information Commissioner.

The Commission’s staff and Records Management

The Commission’s Record Management Policy is available for staff to download from the Intranet, here: http://www.watercommission.co.uk/intranet/view_Staff_Guidance,_Policies__Procedures.aspx. Any new members of staff are prompted to read this document as part of their induction process.

A mini workshop took place on 17 May 2016 with Senior Management to discuss the importance of records management, and what may be required from staff following The Keeper’s acceptance of our plan. In addition to internal workshops, induction training and refresher training will also be rolled out to staff.

Element 4: Business Classification

A business classification scheme describes the business activities the authority undertakes – whether alone or in partnership.

The Commission has a retention policy and a business classification and retention schedule.

This policy document and schedule will support the application of consistent systems and procedures for the management of all records held by The Commission.

The retention policy and schedule will undergo continuous review to ensure The Commission are complying with retention and disposal rules and are in a position to identify and log new records.

Although the Commission has a business classification and retention schedule in place, it is in progress and not yet complete. The Commission aim's to have a complete schedule by 2018 and a robust plan is in place to ensure this target date is reached. A letter of assurance has been sent to The Keeper illustrating our future plan and is available as evidence.

Element 5: Retention Schedules

A retention schedule is a list of records for which pre-determined disposal dates have been established.

The Commission has a retention policy and a business classification and a retention schedule.

These documents outline how long records should be kept and what action should be taken at the end of their lives.

Work has been undergone to review all records, their classification, retention periods and triggers and have been updated as appropriate to align with current business needs.

The retention policy and schedule will both undergo continuous review to ensure The Commission are complying with retention and disposal rules and are in a position to identify and log new records. Although this is currently in draft format, the schedule will be finalised and implemented in 2018.

Going forward, there will be one person in each area of the business with responsibility for ensuring the proper deployment of the schedules and to provide support to records management colleagues in implementing the schedules and retention triggers effectively.

As this element is a work in progress, we have included a work plan which outlines our intention to put in place staff guidance documents and records management training for all members of staff.

RECORDS MANAGEMENT WORK PLAN

This work plan has been developed to ensure the timely implementation of the Water Industry Commission for Scotland's Records Management Plan and to monitor progress in complying with our records management policy.

Timeline	Description of task	Completion Date
End of August 2016	Submission of MOU with NRS	10/08/16
End of October 2016	Business continuity – Review presence and security of vital paper records.	

End of December 2016	Classification and retention schedule complete.	
End of 2016	Internal Audit of records management.	December 2016
End of January 2017	GARP analysis 2017.	28/07/17
End of January 2017	Review and compare Records Management policies and classification and retention schedule to ensure consistency of information.	
End of November	Workshops on naming conventions, file saving and destruction procedures & induction processes for new starts.	
December 2017	Annual Update to Keeper on progress	
End of December 2017	Develop and draft staff guidance.	
End of January 2018	GARP analysis 2018.	
End of February 2018	Staff guidance approved by senior management.	
End of February 2018	Review classification and retention schedule for accuracy/completeness.	
End of March 2018	Staff training plan to be devised.	
End of April 2018	Staff training on records management including roll out of ‘custodian’ and ‘delegated’ asset owner responsibilities.	
End of May 2018	Classification and retention schedule rolled out office wide and implemented (destruction of records/NRS transfer*).	
December 2018	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot	

	checks/review flags any issues, refresher training will be organised for staff).	
December 2018	Annual Update to Keeper on progress	
January 2019	Review of records management policy.	
End of January 2019	GARP analysis 2019	
March 2019	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
June 2019	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
September 2019	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
December 2019	Annual Update to Keeper on progress	
December 2019	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	

January 2020	Review of records management policy.	
March 2020	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff). Update RMP where necessary/required.	
June 2020	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
September 2020	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
December 2020	Annual Update to Keeper on progress	
December 2020	Quarterly review of retention and classification schedule & spot checks on naming conventions and file saving procedures (where spot checks/review flags any issues, refresher training will be organised for staff).	
January 2021	Review of records management policy.	
January 2021 – June 2021	Full review of Records Management Plan and classification and retention schedule. Update RMP where necessary/required.	

July 2021	Records Management Plan reviewed by the Keeper.	

* NRS transfer if applicable – systems for transferring electronic records may not yet be operational with NRS by this date.

Element 6: Destruction Arrangements

It is not always cost-effective or practical for an authority to securely destroy records in-house. Many authorities engage a contractor to destroy records and ensure the process is supervised and documented. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 2 (b) (iii).

Paper Records

The Commission has a contract in place for the bulk destruction of paper records.

Shred It provides us with a confidential shredding service for paper records. This contract allows for Shred It to provide the Commission with onsite secure bins, into which staff can discard confidential papers. These bins are emptied by Shred It on a regular basis, generally once every 6 weeks – as we are a small office, this is more than sufficient.

Following destruction, Shred It provide us with certificates to confirm that our paper records have been successfully and securely destroyed. A copy of these, and our contract is included.

Further information on Shred It can be found here: http://www.shredit.co.uk.

Other evidence of our destruction arrangements are included in our IT Security Policy which has been approved by our Senior Management and Commission Members. This policy has also been through a formal review by our lawyers.

The Commission does not currently keep a record of any paper files that are destroyed. However, appropriate fields will be included in our Classification and Retention Schedule which do capture this going forward.

Electronic Records

On Premise

On premise backup arrangements are in place to allow the recovery of deleted information up to 3 months after deletion. After this time the information is no longer held and cannot be recovered.

Off Premise

Off Premise backup arrangements fall into 2 categories

1. **Sharepoint**
2. **Email**

SharePoint data is held for a maximum 3 months following deletion after which time the information is no longer held and cannot be recovered

Email data is held for a maximum of 44 days following deletion after which time the information is no longer held and cannot be recovered.

Once the Commission has identified any storage device, laptop, PC, server, Hard Disk Drive that is no longer fit for purpose then then all data is removed by the Commission’s IT staff. Arrangements are then made with an external specialist contractor for the safe, secure destruction and environmental disposal of the equipment. Evidence in the form of official destruction certificates are obtained.

The Commission does not currently keep a record of any electronic files that are destroyed. However, appropriate fields will be included in our Classification and Retention Schedule which do capture this going forward.

Element 7: Archiving and Transfer Arrangements

This is a mechanism by which an authority transfers records of enduring value to an appropriate archive repository, specifying the timing of transfers and other terms and conditions. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 2 (b) (iii).

We have obtained final signature from NRS on the MOU to transfer and archive our corporate records. We have included the final, signed MOU and relevant correspondence as evidence.

We have agreed that the records suitable for permanent preservation will include the following:

1. Commission Meeting, agenda, minutes and papers from 2005
2. Annual Reports (these are not held by NLS) from 2005
3. Corporate Plans
4. Major Reports
5. Consultation and reports
6. Methodologies and price review

We will continue to review our records going forward to identify any that may be suitable for transfer to NRS.

Element 8: Information Security

Information security is the process by which an authority protects its records and ensures they remain available. It also maintains privacy where appropriate and provides for the integrity of the records. This is a compulsory element under the terms of the Public Records (Scotland) Act 2011: Section 1 2 (b) (ii).

The Commission does not contract out any of its core functions – everything is done in house. Service Contracts are in place with contractors to aid us in our work, but this is always done alongside a staff member of The Commission.

On Premise Information Security

Physical Security Controls - Access to the Commission's office is controlled by a controlled access fob system. There is a fob system on the building entrance, and again at the Commission's office entrance. Other people who share the building (but not our office) are unable to gain access to the Commission's office unless a staff member physically unlocks the door.

Access to the on premise temperature controlled IT server room is also via the controlled access fob system. There are three people within the Commission who can access the server room – IT Manager, IT Assistant and the Office Manager (in the event of an emergency only).

The building is further protected with CCTV recording in operation. In addition we have an alarm system which is connected to a BT Redcare monitoring system. This notifies Westguard Security in the event of a break in. The formal procedures for Westguard Security is included as evidence.

All on premise hardware which has been used to store the Commission's data is destroyed once it is no longer fit for purpose. The destruction is outsourced to an industry expert and proof of destruction certificates are obtained.

The Commission's on premise IT systems are further protected by securing the PC's to the desk frames using industry standard Kensington lock security cables.

Logical Security Controls

The Commission on premise data is protected via an Internet Gateway firewall service which prevents unauthorised access from external threats. The data is also protected using multi-layer security software, this protects the data at the Gateway, Servers and endpoint systems from malicious attacks such as virus, malware, phishing etc.

Data Security Controls

Access to the Commission's on premise data is provided to staff via Windows Active Directory domain based authentication (user names and passwords). This provides users with access to only the system resources they require access to using permissions to allow and deny access control. Remote access to the Commission on premise IT systems is provided via an encrypted mobile device e.g. laptop.
All passwords are controlled by the Domain policy used to access the Commission's systems and are configured to be complex and force a change at set intervals.

Admin Controls

Administrative controls to the system are restricted to the IT team

On Premise Backups

Backups are performed and rotated on a daily, weekly and monthly basis and retained for a maximum 3 month period. The backups are used for file recovery and to support the Commission's Disaster Recovery and Business Continuity plans. The disks are collected, delivered, transported and stored using a third party secure disk storage contractor. We use a contractor called Dataspace to manage and store our disks. You can find information on Dataspace here: http://www.dataspacescotland.co.uk, and our contract with them is included as evidence.

Cloud Based Information Security

The Commission also store data in Microsoft Office 365 cloud platform. This is used for saving data in SharePoint Online and for Email services.

Office 365 is a security-hardened service, designed following the Microsoft Security Development Lifecycle.

At the service level, Office 365 uses the defence-in-depth approach to provide physical, logical, and data layers of security features and operational best practices. In addition, Office 365 provides enterprise-grade, user and admin controls to further secure the environment.

Physical security

- 24-hour monitoring of data centres.
- Multi-factor authentication, including biometric scanning for data centre access.
- Internal data centre network is segregated from the external network.
- Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- Faulty drives and hardware are demagnetized and destroyed.

Logical security

- Lock box processes for strictly supervised escalation process greatly limits human access to your data.
- Servers run only processes on whitelist, minimizing risk from malicious code.
- Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.
- Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

Data security

- Encryption at rest protects your data on our servers.
- Encryption in transit with SSL/TLS protects your data transmitted between you and Microsoft.
- Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.

Admin and user controls

Rights Management Services prevents file-level access without the right user credentials.

Off Premise Backups

Microsoft Office 365 provides multiple layers of redundancy and backups of information at the datacentre level, so in a rare event where data may be lost or corrupted on Microsoft servers, it can be restored. This data is further protected by Microsoft who also replicate the data at the data centre level to another data centre at a different location therefore providing geo location level redundancy. The Office 365 services are available with a guaranteed 99.9% uptime, financially backed service level agreement (SLA). More detailed information is available here https://products.office.com/en-us/business/office-365-for-business-support-options

IT Policies

All new staff are given a copy of our *IT Systems Acceptable Use and Notice of Monitoring Policy* which they must read and sign to say they have understood, before any IT access is granted to our systems. A copy of this signed policy is retained in the employee’s personnel file.

All of our policies are subject to regular review and were reviewed by our lawyers, Harper McLeod in March 2016. Updated versions of these policies are published on our intranet and staff are also sent the updated policies via email and encouraged to make themselves familiar with their content. Such policies include: Information Technology Security Policy, Ipad Iphone Policy, IT Systems Acceptable Use and Notice of Monitoring Policy, Risk Management Policy, Data Protection Policy.

Element 9: Data Protection

An authority that handles personal information about individuals has a number of legal obligations to protect that information under the Data Protection Act 1998.

The Commission recognises the importance of ensuring that Personal Data is handled in accordance with the Data Protection Principles set out in the Data Protection Act 1998. Failure by Commission employees to safeguard Personal Data properly might result in disciplinary action being taken.

The Commission's principal purposes for holding Personal Data on personnel files are:

- recruitment, promotion, training, pension, sickness records, pension forms, redeployment and/or career development;
- the calculation of payroll data and the transfer of such data for use by financial employees and independent auditors;
- the determination and calculation of certain benefits, including superannuation;
- for contacting next of kin and arranging medical attention in connection with an emergency at work;
- prevention of fraud;
- compliance with lawful requests from government agencies;
- disciplinary or capability information arising from an employee's conduct, or ability to perform their job requirements; and
- the provision of references/reports to third parties on request.

The Commission has a Data Protection Policy which sets out the approach taken by the Commission on data protection legislation.

All staff can view and download the Data Protection Policy from our Intranet here: http://www.watercommission.co.uk/intranet/UserFiles/Documents/Data%20Protection%202016.pdf. Any new staff are also given a copy of this as part of their induction.

The Commission is registered with the Scottish Information Commission and our current registration is valid until 17 February 2017. Our registration number is: Z2094773.

The Commission has one FoI exemption which relates to information about our Final Determination. The exemption allows us to hold off releasing any information until after the Final Determination has been published i.e. anything that is in draft form. A guidance document is include as evidence.

Element 10: Business Continuity and Vital Records

A business continuity and vital records plan serves as the main resource for the preparation for, response to, and recovery from, an emergency that might affect any number of crucial functions in an authority.

The Commission has a Business Continuity Plan. The purpose of this plan is to ensure that there is no significant disruption to the services provided by the Commission. It is to ensure that essential needs of the Commission's stakeholders continue to be met in the event of failure of, or disruption to, facilities.

The Emergency Co-ordination Team consist of the following people:

- Director of Corporate Affairs & Strategy
- Office Manager
- Financial Controller
- IT Manager
- IT Assistant
- Communications Officer

This team has responsibility for:

- Managing the crisis
- Liaising with staff and partner organisations
- Communication during the crisis
- Overseeing the restoration of business critical functions
- Returning operations to 'normal'
- Liaising regarding IT recovery
- Allocating tasks to appropriate staff members to implement the recovery plan

Our Business Continuity Plan has been reviewed by our lawyers and our Audit Committee and is available to all staff via our intranet.

The Emergency Co-ordination Team have undergone numerous training sessions on incident management, with Plan B Consulting.

In the event of a disaster occurring which impacts any electronic records stored on the Commission's on premise systems, the Commission have in place an IT technical recovery procedure. This enables the full recovery of the on premise network and server systems that contain the on premise data and records. The full on premise network and data can be recovered and be accessible within 24 hours. A contract with an external Disaster Recover contractor ITFA Ltd exists to provide the recovery services at their offices in Grangemouth. An unannounced annual IT recovery test is performed to ensure this works as expected and any issues or recommendations for improvement are identified and considered.

In the event of a disaster occurring which impacts any electronic records stored on the Commission’s off premise systems (Microsoft Office 365 cloud platform), then this is protected by the 99.9% SLA and robust resilience and contingency measures included in this service.

The Commission does not have any procedures in place to protect vital paper records. There is not a large volume of paper records that would be considered vital, however, we will review this as part of our ongoing records management work plan.

Element 11: Audit Trail

An audit trail is a sequence of steps documenting the movement and/or editing of a record resulting from activities by individuals, systems or other entities.

Paper Records

On a daily basis we receive mail into our office which is logged on our mail logging system before being scanned and saved to SharePoint. We file all incoming and outgoing mail in the office and dispose of as per our retention schedule.

Other than mail, we only hold corporate records in a paper form of personnel records and financial records. Sensitive personnel files and financial files are stored in locked cupboards and are only accessible to the Office Manager (personnel) and the Financial Controller and Finance Officer (personnel and finance). Disposal of such records takes place in accordance with our retention schedule.

Electronic Records

On Premise:

Records are stored in a network file share which has a categorised file structure based on the Commission's business areas. Access to the data is controlled through Microsoft Windows Active Directory/Directory Services, which utilises industry standard security controls to ensure only staff with valid usernames and passwords can access the data and only data that they have been granted permission to. Permissions are restricted at a file and folder level, depending on the business area, i.e. only members of the Finance Group are able to access the Finance data.
All the data in this network file share has been restricted to read only (subject to having the appropriate read only access) and is now used as an archive reference as the Commission transitions from on premise systems to cloud based services. The remaining "Live" on premise data held by the Commission is financial data. This data is only accessible to 2 members of the Finance team. In addition to Microsoft Windows access controls the finance team also require additional application level username and passwords to access the financial data. Further detailed audit reports are available within the financial application software which provide details of all the transactions.

Off Premise:

In 2015 we moved our file structure onto a cloud based SharePoint platform which is part of Office 365. SharePoint provides the ability to track the creation, deletion and modification of electronic documents.

Audit trail settings within SharePoint enables administrators to keep a reliable log of what is happening with important content on a site. Administrators are able to retrieve a rolling 90day history of actions taken by a particular user, or all users. Knowing who has done what with information is critical for regulatory compliance and records management. Reports can be captured, customised and printed using Microsoft Office Excel.

Naming Conventions

The Commission does not currently enforce any strict naming conventions on any files however, this is something that we will review as part of our ongoing records management work plan. Detail on how staff are expected to name their files will become part of The Commission’s corporate style guidance, which will be available to view on the Intranet once completed.

Element 12: Competency Framework for Records Management Staff

A competency framework lists the core competencies and the key knowledge and skills required by a records manager. It can be used as a basis for developing job specifications, identifying training needs, and assessing performance.

The Commission's size and budget does not allow it to have an individual post dedicated to records management. Instead, records management is included as a specific dimension in the job description of the Finance Officer & PA.

Training has been identified by PDP Training and a two day course took place on 20 and 21 April 2016. This training was provided to three members of staff to ensure there was sufficient back up of resources. Further training will be sought for all staff where necessary to ensure the successful and continuous implementation of records management throughout the organisation.

The Commission has a competency framework in place under which staff performance is measured against work-related objectives on an annual basis. Therefore, work related objectives specific to records management, as well as continuing professional development, are a formal element of the Records Officer's annual appraisal.

Element 13: Assessment and Review

Regular assessment and review of records management systems will give an authority a clear statement of the extent that its records management practices conform to the Records Management Plan as submitted and agreed by The Keeper.

The Records Manager will work alongside the other team members to ensure The Commission’s records management plan and related policies are reviewed regularly. Review progress will be reported to the Director of Corporate Affairs & Strategy who has overall responsibility for Records Management.

A GARP (Generally Accepted Records Keeping Principles) Analysis has been carried out to illustrate the current position within The Commission and how Records Management is being dealt with. This chart is included as evidence. A GARP analysis will be done once per year to capture progress made by the Commission.

The Commission will use their Internal Auditors to carry out a full review of their Records Management process following acceptance of their Records Management Plan by The Keeper. They will then aim to have subsequent partial reviews in order to alleviate any potential future breaches. The Internal Auditors have provided a draft plan for the period 2016-17 which illustrates the Records Management Review scheduled for this year.

Our ongoing records management work plan has been included as evidence which outlines our plans for assessment and review going forward.

Element 14: Shared Information

Under certain conditions, information given in confidence may be shared. Most commonly this relates to personal information, but it can also happen with confidential corporate records.

Where data sharing takes place, it is carried out in line with the Data Protection Act 1998 and other relevant privacy information. Sharing of information is allowed only after an appropriate risk assessment has been carried out.

As outlined earlier in this document, under Data Protection legislation, the Commission is required to register as a data controller with the Information Commissioner. This requires the Commission to stipulate, amongst other things, with whom it will or is likely to share data.

We sometimes need to share the personal information we process with other organisations. Where this is necessary we are required to comply with all aspects of the Data Protection Act 1998 (DPA). What follows is a description of the types of organisations we may need to share some of the personal information we process with, for one or more reasons. Where necessary or required we share information with:

- data subjects (employees, suppliers, complainants or their representatives);
- suppliers;
- current, past or prospective employers;
- persons making an enquiry or complaint; and
- other ombudsman and regulatory authorities.

The Commission has a number of agreements with other organisations. In most cases these agreements formalise, in a general sense, the data that can be and is shared between them on a regular and ongoing basis.

The main source of information sharing by The Commission is with Scottish Water. Any information being given to Scottish Water, or being received from Scottish Water, is done so via a ‘Monitoring’ mailbox. This Monitoring mailbox is checked regularly and on a daily basis.

Annex A: Evidence

Element 1: Covering letter from Alan Sutherland, Chief Executive and Katherine Russell, Director of Corporate Affairs and Strategy.

Element 2: Covering letter from Alan Sutherland, Chief Executive and Katherine Russell, Director of Corporate Affairs and Strategy. Finance Officer & PA job description. Training course documentation x2.

Element 3: WICS Records Management Policy. Screen shot of Intranet download availability. Workshop documentation.

Element 4: Retention Policy. Classification and Retention Schedule. File Plan. Letter of assurance from DCA. Screen shot of Intranet download availability. Ongoing Records Management Work Plan.

Element 5: Retention Policy. Classification and Retention Schedule. Letter of assurance from DCA. Ongoing Records Management Work Plan.

Element 6: Retention Policy. Classification and Retention Schedule. Shred It destruction certificates x5. Shred It contract. Dataspace contract. Dataspace destruction certificate. IT Security Policy. Screen shot of Intranet download availability. IT obsolete inventory list. MGH Scotland destruction certificate. SEPA Destruction certificate.

Element 7: Correspondence between WICS and NRS regarding draft MOU. Draft MOU between WICS and NRS. Final approved MOU between WICS and NRS.

Element 8: Information Technology Security Policy. Ipad Iphone Policy. IT Systems Acceptable Use and Notice of Monitoring Policy. Dataspace contract. Dataspace destruction certificate. Westguard Security Procedures. Screen shot of Intranet download availability. IT obsolete inventory list. MGH Scotland destruction certificate. SEPA Destruction certificate.

Element 9: Data Protection Policy. Registration with Information Commissioner x2. Details of FOI exemption. Screen shot of Intranet download availability.

Element 10: Business Continuity Plan. ITFA DR Contract (15-16 and 16-17). Ongoing Records Management Work Plan. Classification and Retention Schedule.

Element 11: Permissions screen shot from Sage. Audit report from Sage. Screen shot of SharePoint audit trail function. Screen shot of Z Drive locked down status. Ongoing Records Management Work Plan.

Element 12: Finance Officer & PA job description. PDP training course detail x2. Civil Service Learning Record. Workshop Paperwork.

Element 13: GARP Analysis 2016. Draft Internal Audit Review Plan 2016-17. Ongoing Records Management Work Plan.

Element 14: Screen shot of Monitoring Mailbox. Screen shot of email correspondence with Scottish Water. Registration with Information Commissioner x2. Screen shot of Intranet download availability.